9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2021-0004]

Privacy Act of 1974; System of Records

AGENCY: Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.

ACTION: Notice of a New System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "DHS/Cybersecurity and Infrastructure Security Agency (CISA)-005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records." This system of records allows DHS/CISA ("Agency") to receive and collect customer or subscriber contact information from electronic communications service providers to identify and notify entities at risk of security vulnerabilities relating to critical infrastructure information systems and devices. This newly established system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This new system will be effective upon publication. Routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may submit comments, identified by docket number CISA-2021-0004 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number CISA-2021-0004. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT:

For general questions, please contact: James Burd, (703) 235-1919, Privacy@cisa.dhs.gov, Chief Privacy Officer, Office of the Privacy Office, Cybersecurity and Infrastructure Security Agency, Washington, D.C. 20528-0655. For privacy questions, please contact: Lynn Parker Dupree, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) proposes to establish a new CISA system of records entitled, "DHS/CISA-Administrative Subpoenas for Cybersecurity Vulnerability Identification System of Records." Subsection (o) of Section 2209 of the Homeland Security Act, as amended, 6 U.S.C. sec. 659(o), grants CISA the authority to issue a subpoena for the production of information necessary to identify and notify an entity at risk, where the entity owns or operates what CISA has reason to believe is a "covered device or system"[1]

[1] "Covered device or system" means a device or system commonly used to perform industrial, commercial, scientific, or government functions or processes related to critical infrastructure, including operational and

with a specific security vulnerability relating to critical infrastructure, and if CISA itself is unable to identify the entity at risk that owns or operates such covered device or system. CISA will issue subpoenas to providers of public electronic communications services, such as Internet Service Providers (ISP), that have relevant customer or subscriber information to identify the owners or operators of covered devices or systems with a specific security vulnerability, often identified through their internet protocol (IP) address. The Electronic Communications Privacy Act of 1986 (18 U.S.C. sec. 2510 et seq.) permits the federal government to subpoena such service providers for basic subscriber information. The information to be collected by CISA is not for intelligence or prosecution activities, but rather to notify entities of potential cybersecurity risks to covered devices or systems with a specific security vulnerability relating to critical infrastructure.

This system of records will cover records of individuals identified in the information provided by the ISP as the owner or operator of a covered device or system connected to the internet with a specific security vulnerability related to critical infrastructure. CISA maintains this information to identify and notify the individual of the vulnerability on the covered device or system.[2]

This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is

---

industrial control systems, distributed control systems, and programmable logic controllers. The term "covered device or system" does not include personal devices or systems, such as consumer mobile devices, home computers, residential wireless routers, or residential internet enabled consumer devices. *See* 6 U.S.C. sec. 659(o)(1).

[2] Pursuant to 6 U.S.C. sec. 659(o)(8), the Agency may not require an owner or operator of critical infrastructure to take any action as a result of a notice of vulnerability made pursuant to 6 U.S.C. 659(o).

maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/CISA-005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: DHS/CISA-005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification.

SECURITY CLASSIFICATION: Controlled Unclassified Information

SYSTEM LOCATION: Records are maintained at CISA locations such as Arlington, Virginia and Pensacola, Florida.

SYSTEM MANAGER(S): Division Director, National Cybersecurity and Communications Integration Center (NCCIC) Hunt & Incident Response, 1110 North Glebe Rd. Arlington, VA 22201.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Subsection (o) of Section 2209 of the Homeland Security Act, as amended, 6 U.S.C. sec. 659(o).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to maintain records for the purpose of identifying and notifying entities at risk of security vulnerabilities relating to critical infrastructure on covered devices and systems. The authority is available only in circumstances where CISA knows of a specific cybersecurity risk to a covered device or system but is unable to determine the owner or operator of the covered device or system. The information sought by subpoena is limited to only basic categories of subscriber information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individual(s) whose contact information is provided by an electronic communication service provider in response to a subpoena as described above.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of records in this system include the following information obtained through subpoenas:

- Name;
- Address;
- Length of service (including start date) and types of service utilized; and
- Telephone or instrument number or other subscriber number or identity.

In addition, the system will also include the following categories of records:

- IP address;
- Individual's position/title or organizational affiliations; and
- Identifier or ticket number created by CISA to retrieve information.

RECORD SOURCE CATEGORIES: Information is obtained from a subpoenaed individual, partnership, corporation, association, or entity. Information may also be obtained through public sources or contact with an individual identified through the issuing of a subpoena.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In accordance with subsection (o) of Section 2209 of the Homeland Security Act, as amended, (6 U.S.C. sec. 659(o)), the Agency may not disseminate nonpublic information obtained through a subpoena that identifies the party that is subject to such subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information with the Department of Justice for the purpose of enforcing such subpoena in non-compliance circumstances, and may share with a federal agency the nonpublic information of the entity at risk if the requirements of 6 U.S.C. sec. 659(o)(7)(A) are met so long it is used by that federal agency for a cybersecurity purpose, as defined in 6 U.S.C. sec. 1501, in accordance with 6 U.S.C. sec. 659(o)(12).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: CISA will retrieve records by CISA-created ticket number associated with a covered device or system connected to the internet identified as having a security vulnerability. Records may also be retrieved by IP address or phone number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records that are stored in an individual's file will be purged according to the retention and disposition guidelines under 6 U.S.C. sec. 659(o)(7)(C)(ii), which requires destruction of any personally identifiable information not later than six (6) months after the date on which the Agency receives information obtained through subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent. CISA is developing a records retention schedule for submission and approval by the National Archives Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: CISA safeguards records in this system according to applicable rules and policies, including all applicable CISA automated systems security and access policies. CISA has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those CISA officials who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the DHS Chief Privacy Officer or the appropriate Headquarters or component's FOIA Officer whose contact information can be found at https://www.dhs.gov/freedom-information-act-foia under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the DHS Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or

correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

*****

Lynn Parker Dupree,

Chief Privacy Officer,

U.S. Department of Homeland Security.

[FR Doc. 2021-06874 Filed: 4/2/2021 8:45 am; Publication Date: 4/5/2021]